Deutscher Bundestag **Drucksache 19/27071**

19. Wahlperiode 25.02.2021

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Oliver Luksic, Frank Sitta, Bernd Reuther, weiterer Abgeordneter und der Fraktion der FDP
– Drucksache 19/26126 –

KRITIS (Kritische Infrastrukturen) in der Verkehrs- und digitalen Infrastruktur

Vorbemerkung der Fragesteller

Vernetzung und Digitalisierung bieten viele Vorteile und Fortschritte, gerade in Bezug auf die zugrunde liegende digitale Infrastruktur und die durch sie möglichen Anwendungen im Rahmen der Verkehrsinfrastruktur. Mit der fortschreitenden Digitalisierung wachsen allerdings auch die Abhängigkeit und die Anfälligkeit der bestehenden Systeme. Besondere Bedeutung haben in dieser Hinsicht Teile der sogenannten Kritischen Infrastruktur, wie sie die EU-Richtlinie 2008/114/EG festlegt, die wichtige gesellschaftliche Funktionen wie die Versorgung der Bevölkerung, die interne Kommunikation oder die Verteidigungsbereitschaft des Landes betreffen. Ein teilweiser Ausfall oder gar Absturz Kritischer Infrastrukturen kann daher schwerste Auswirkungen auf das Leben in der Bundesrepublik haben. Das Bundesministerium des Innern, für Bau und Heimat ist daher gemeinsam mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe federführend am Schutz dieser Kritischen Infrastrukturen beteiligt.

1. Welche Teile der Verkehrsinfrastruktur im Saarland sind nach Kenntnis der Bundesregierung Teil der Kritischen Infrastruktur, wie sie die BSI-Kritisverordnung regelt?

2. Welche Teile der Verkehrsinfrastruktur in Nordrhein-Westfalen sind nach Kenntnis der Bundesregierung Teil der Kritischen Infrastruktur, wie sie die BSI-Kritisverordnung regelt?

Die Fragen 1 und 2 werden aufgrund ihres Sachzusammenhangs gemeinsam beantwortet.

Die erbetenen Informationen zu Kritischer Infrastrukturen – insbesondere in dieser Detailebene – können nicht öffentlich zur Verfügung gestellt werden. Unbefugte würden die Möglichkeit erhalten, aus diesen Daten Rückschlüsse zu ziehen, die einzeln oder in ihrer Kombination eine Gefahr für Einrichtungen der Kritischen Infrastrukturen alleine oder in der Gesamtheit darstellen. Durch eine

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums für Verkehr und digitale Infrastruktur vom 25. Februar 2021 übermittelt.
Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

Ableitung aus Anzahl und Teilbereichen ließen sich anhand von Land und Bekanntheitsgrad einer Infrastruktur/eines Unternehmen Rückschlüsse auf die Kritische Infrastruktur ziehen.

Unter Abwägung zwischen dem parlamentarischen Auskunftsanspruch einerseits und dem Schutz von Sicherheitsinteressen der Bundesrepublik Deutschland mit Berücksichtigung der Geheimhaltung von Informationen zu Kritischen Infrastrukturen andererseits hat die Bundesregierung die erbetenen Informationen als Verschlusssache „VS – Vertraulich – amtlich geheimgehalten“ eingestuft und der Geheimschutzstelle des Deutschen Bundestages übermittelt. Die Antwort der Bundesregierung ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung des Deutschen Bundestages eingesehen werden.

3. Wie viele Anlagen oder Systeme der Kritischen Infrastruktur gibt es in den folgenden, im Anhang 7 der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz festgelegten, Kategorien (bitte jeweils für Gesamtkategorien und Unterkategorien beantworten):

   a) Luftverkehr insgesamt,
      - Anlage oder System zur Passagierabfertigung an Flugplätzen,
      - Anlage oder System zur Frachtabfertigung an Flugplätzen,
      - Infrastrukturbetrieb eines Flugplatzes,
      - Flugsicherung und Luftverkehrskontrolle,

   b) Schienenverkehr insgesamt,
      - Personenbahnhof der Eisenbahn,
      - Güterbahnhof,
      - Zugbildungsbahnhof,
      - Schienennetz und Stellwerke der Eisenbahn,
      - Verkehrssteuerungs- und Leitsystem der Eisenbahn,
      - Leitzentrale der Eisenbahn,

   c) See- und Binnenschifffahrt insgesamt
      - Anlage oder System zum Betrieb von Bundeswasserstraßen,
      - Verkehrssteuerungs- und Leitsystem der See- und Binnenschifffahrt,
      - Leitzentrale von Betreibern und Verkehrsunternehmen der Seeschifffahrt,
      - Anlage oder System zur Disposition von Binnenschiffen (nur Güterverkehr),

   d) Straßenverkehr insgesamt,
      - Verkehrssteuerungs- und Leitsystem,
      - Verkehrssteuerungs- und Leitsystem im kommunalen Straßenverkehr,

   e) Öffentlichen Personennahverkehr (ÖPNV) insgesamt,
      - Schienennetz und Stellwerke des öffentlichen Straßenpersonenverkehrs (ÖSPV),
      - Verkehrssteuerungs- und Leitsystem des ÖPNV,
      - Leitzentrale des ÖSPV (Betreiber, Verkehrsunternehmen),

f) Logistik insgesamt,

- Anlage oder System zum Betrieb eines Logistikzentrums in den Segmenten Massengut-, Ladungs-, Stückgut-, Kontrakt-, See- oder Luftfrachtlogistik,
- Anlage oder IT-System zur Logistiksteuerung oder Logistikverwaltung in den Segmenten Massengut-, Ladungs-, Stückgut-, Kontrakt-, See- oder Luftfrachtlogistik,

g) Sonstige insgesamt,

- Anlage zur Wettervorhersage, zur Gezeitenvorhersage oder zur Wasserstandsmeldung,
- Satellitennavigationssystem,

h) Informationstechnik und Telekommunikation insgesamt,

- Ortsgebundenes Zugangsnetz,
- Übertragungsnetz,
- IXP,
- DNS-Resolver, die zur Nutzung öffentlich zugänglicher Telefondienste, Datenübermittlungsdienste oder Internetzugangsdienste angeboten werden,
- Autoritative DNS-Server,
- Rechenzentren (Housing),
- Serverfarmen (Hosting),
- Content Delivery Netzwerke,
- Anlagen zur Erbringung von Vertrauensdiensten?

4. Welche der vorgenannten Anlagen oder Systeme sind nach Kenntnis der Bundesregierung ausreichend (so wie es die BSI-Kritisverordnung vorsieht) geschützt (bitte nach genutzten Parametern sowie nach ausreichend und nicht ausreichend aufschlüsseln)?

Die Fragen 3 und 4 werden aufgrund ihres Sachzusammenhangs gemeinsam beantwortet.

Betreiber Kritischer Infrastrukturen sind gemäß § 8a Abs. 1 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) in Verbindung mit der BSI-Kritisverordnung verpflichtet, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind.

Das Gesetz fordert nach § 8a Abs. 3 BSIG die Betreiber Kritischer Infrastrukturen auf,

mindestens alle zwei Jahre die Erfüllung der Anforderungen nach Absatz 1 auf geeignete Weise nachzuweisen. Der Nachweis kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen. Die Betreiber übermitteln dem Bundesamt für Sicherheit in der Informationstechnik (BSI) die Ergebnisse der durchgeführten Audits, Prüfungen oder Zertifizierungen einschließlich der dabei aufgedeckten Sicherheitsmängel.

Die Beantwortung dieser Fragen erfolgte nach folgenden Maßgaben:

- Die Bundesregierung betrachtet Anlagen als im Sinne der Frage ausreichend geschützt, wenn der Betreiber dieser Infrastruktur einen Nachweis gemäß § 8a Abs. 3 BSIG erbracht hat.

- Die Bundesregierung betrachtet Anlagen als im Sinne der Frage nicht ausreichend geschützt, wenn bei der Übermittlung von mindestens einem erheblichen Mangel deutlich wurde, dass teilweise noch zusätzliche Maßnahmen umgesetzt werden müssen, und das BSI über den Abschluss dieser Maßnahmen nicht informiert wurde. Das BSI erhielt von den Unternehmen einen Plan zur Abstellung der Mängel. Die Unternehmen setzen diesen um.

Im Übrigen können die erbetenen Informationen zu Kritischen Infrastrukturen – insbesondere in dieser Detailebene – nicht öffentlich zur Verfügung gestellt werden. Unbefugte würden die Möglichkeit erhalten, aus diesen Daten Rückschlüsse zu ziehen, die einzeln oder in ihrer Kombination eine Gefahr für Einrichtungen der Kritischen Infrastrukturen alleine oder in der Gesamtheit darstellen.

Die Übersicht über den Stand der IT-Sicherung im Bereich Transport und Verkehr lässt diverse Schlüsse auf nicht hinreichend nachgewiesene Absicherung von Kritischen Infrastrukturen zu. Die Kenntnisnahme durch Unbefugte ist für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder nachteilig.

Unter Abwägung zwischen dem parlamentarischen Auskunftsanspruch einerseits und dem Schutz von Sicherheitsinteressen der Bundesrepublik Deutschland mit Berücksichtigung der Geheimhaltung von Informationen zu Kritischen Infrastrukturen andererseits hat die Bundesregierung die erbetenen Informationen als Verschlusssache „VS – Vertraulich – amtlich geheimgehalten“ eingestuft. Die Antwort der Bundesregierung ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung des Deutschen Bundestages eingesehen werden.

5. Welche bundeseigenen Unternehmen betreiben nach Kenntnis der Bundesregierung Anlagen oder Maschinen Teile der Kritischen Infrastruktur, wie sie die BSI-Kritisverordnung regelt?

Die erbetenen Informationen zu Kritischen Infrastrukturen – insbesondere in dieser Detailebene – können nicht öffentlich zur Verfügung gestellt werden. Unbefugte würden die Möglichkeit erhalten, aus diesen Daten Rückschlüsse zu ziehen, die einzeln oder in ihrer Kombination eine Gefahr für Einrichtungen der Kritischen Infrastrukturen alleine oder in der Gesamtheit darstellen. Durch eine Ableitung aus Anzahl und Teilbereichen ließen sich anhand von Land und Bekanntheitsgrad einer Infrastruktur/eines Unternehmen Rückschlüsse auf die Kritische Infrastruktur ziehen.

Unter Abwägung zwischen dem parlamentarischen Auskunftsanspruch einerseits und dem Schutz von Sicherheitsinteressen der Bundesrepublik Deutschland unter Berücksichtigung der Geheimhaltung von Informationen zu Kritischen Infrastrukturen andererseits hat die Bundesregierung die erbetenen Informationen als Verschlusssache „VS – Vertraulich – amtlich geheimgehalten“ eingestuft. Die Antwort der Bundesregierung ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung des Deutschen Bundestages eingesehen werden.

6. Welche Maßnahmen hat die Bundesregierung seit Inkrafttreten der Kritis-Verordnung getroffen, um Kritische Infrastruktur in den der Verkehrs- und digitalen Infrastruktur zu schützen (bitte nach Maßnahmen auflisten)?

Bereits vor der Verabschiedung des IT-Sicherheitsgesetzes wurden Maßnahmen zum Schutz Kritischer Infrastrukturen getroffen, zum Beispiel die „Nationale Strategie zum Schutz Kritischer Infrastrukturen“ und die Gründung des UP KRITIS, eine noch heute bestehende öffentlich-privaten Partnerschaft zum Schutz Kritischer Infrastrukturen.

Im aktuellen IT-Sicherheitsgesetz ist eine Vielzahl von Maßnahmen festgelegt, die sich in die folgenden Kategorien unterteilen lassen:

- Die Pflicht zur Umsetzung von z. B. technischen und organisatorischen Maßnahmen zum Schutz Kritischer Infrastrukturen durch die Betreiber der Kritischen Infrastrukturen,
- die Prüfung der Effektivität der von den Betreibern umgesetzten Maßnahmen durch unabhängige Prüfer oder gemäß § 8a Absatz 4 BSIG durch das BSI,
- Erstellung branchenspezifischer Sicherheitsstandards durch Betreiber Kritischer Infrastruktur und Eignungsprüfung dieser Standards durch das BSI,
- der Aufbau eines Melde- und Informationswesens, durch welches Betreiber Kritischer Infrastrukturen stets über die aktuelle IT-Sicherheitslage sowie akute Risiken und Möglichkeiten der Mitigation informiert werden,
- der Auf- und Ausbau des BSI als Aufsichtsbehörde über die IT-Sicherheit Kritischer Infrastrukturen, um die Einhaltung der Pflichten der KRITIS-Betreiber (wie z. B. Nachweiserbringung oder Meldung von Sicherheitsvorfällen) zu gewährleisten.

Zu nennen ist weiterhin die KRITIS-Betreuung (allgemeine Beratung und Unterstützung Kritischer Infrastrukturen gemäß § 3 Absatz 3 BSIG). Dabei umfasst die Betreuung von KRITIS-Betreibern, auch derer, die unterhalb der Schwellenwerte nach BSI-KritisV liegen, folgende Tätigkeitsbereiche:

- Die Bereitstellung von Orientierungshilfen, Leitlinien, Empfehlungen, Auslegungshilfen und Anwendungshinweisen zur Umsetzung der abstrakten Vorgaben des BSIG:
  - Die Durchführung von Informationsveranstaltungen und Workshops für KRITIS-Betreiber, entweder durch das BSI selbst, über den UP KRITIS, über die Allianz für Cybersicherheit oder im Rahmen von Tagungen und Veranstaltungen von KRITIS-relevanten Verbänden, Gremien oder sonstigen Veranstaltern.
  - Die Beantwortung von individuellen Anfragen von KRITIS-Betreibern zu Problemen, die sich bei der Umsetzung des BSIG ergeben, und die Diskussion von Lösungsmöglichkeiten.
  - Austausch mit einzelnen oder Gruppen von KRITIS-Betreibern, um aktuelle Vorhaben, Herausforderungen und mögliche Lösungen zu besprechen.

Im Sektor Transport und Verkehr bietet das BSI branchenspezifische, bedarfsgerechte Unterstützung in den zuvor genannten Formaten an. Konkrete Beispiele zu den o. g. Punkten sind:

- Unterstützung bei der Erstellung sowie Feststellung der Eignung von branchenspezifischen Sicherheitsstandards,

- Unterstützung bei der Erstellung von IT-Grundschutz-Profilen, z. B. für Reedereien, die nun als internationale Vorgaben auf nationaler Ebene umgesetzt werden können (ISM-Cyber-Security-Rundschreiben),
- Abschluss einer Kooperationsvereinbarung mit der EASA,
- intensiver regelmäßiger Fachaustausch in Kooperation mit Branchenverbänden bzw. anderen zuständigen Aufsichtsbehörden.

7. Welche bundeseigenen Unternehmen erfüllen die bestehenden Sicherheitsstandards, wie sie die BSI-Kritisverordnung regelt, nach Kenntnis der Bundesregierung bisher nicht, und wenn ja, welche Mängel wurden festgestellt?

Zu einzelnen Anlagen darf die Bundesregierung keine Auskunft geben, da dem nach § 8e Absatz 1 BSIG schutzwürdige Interessen des Betreibers dieser Kritischer Infrastrukturen entgegenstehen.

8. Gab es seit Inkrafttreten der Kritis-Verordnung Vorfälle nach § 8b des BSI-Gesetzes in Bezug auf Kritische Infrastrukturen in der digitalen oder Verkehrsinfrastruktur sowie bei bundeseigenen Unternehmen, die der zentralen Meldestelle für Betreiber beim BSI mitgeteilt wurden, und wenn ja, was fiel vor (bitte einzeln und detailliert erklären)?

Die erbetenen Informationen zu möglichen Vorfällen nach § 8b BSIG können nicht öffentlich zur Verfügung gestellt werden. Unbefugte würden die Möglichkeit erhalten, aus diesen Daten Rückschlüsse zu ziehen, die einzeln oder in ihrer Kombination eine Gefahr für Einrichtungen der Kritischen Infrastrukturen alleine oder in der Gesamtheit darstellen. Aus der öffentlichen Nennung des Cyberangriffs ließe sich in Verbindung mit Pressemitteilungen eine Zuordnung zu einzelnen Betreibern Kritischer Infrastrukturen herleiten.

Unter Abwägung zwischen dem parlamentarischen Auskunftsanspruch einerseits und dem Schutz von Sicherheitsinteressen der Bundesrepublik Deutschland unter Berücksichtigung der Geheimhaltung von Informationen zu Kritischen Infrastrukturen andererseits hat die Bundesregierung die erbetenen Informationen als Verschlusssache „VS –Vertraulich – amtlich geheimgehalten“. Die Antwort der Bundesregierung ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung des Deutschen Bundestages eingesehen werden.

9. Wie viele Betreiber Kritischer Infrastrukturen haben nach Kenntnis der Bundesregierung noch nicht die im BSI-Gesetz festgelegten Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit getroffen, und wie viele Betreiber sind noch im Aufbau von Informationssicherheitsmanagementsystemen (ISMS) nach ISO 27001?

Alle Betreiber, die dem BSI einen Nachweis erbracht haben, haben entsprechende Vorkehrungen getroffen. Zu Betreibern, die keinen Nachweis erbracht haben, liegen der Bundesregierung keine Erkenntnisse vor. Im Zuge der Nachweiserbringung erhält das BSI Kenntnis über die von der Prüfstelle genutzte Prüfgrundlage. Ein Rückschluss auf den vom Betreiber genutzten Standard, wie z. B. ISO 27001, kann daraus nicht zwingend gezogen werden.

Entsprechend liegen dazu keine Daten vor.

Die erbetenen Informationen zur Nennung von Betreibern können nicht öffentlich zur Verfügung gestellt werden. Unbefugte würden die Möglichkeit erhalten, aus diesen Daten Rückschlüsse zu ziehen, die einzeln oder in ihrer Kombination eine Gefahr für Einrichtungen der Kritischen Infrastrukturen alleine oder in der Gesamtheit darstellen.

Die Kennzahlen der Anlagen ohne Nachweis ermöglichen eine Einschätzung der IT-Sicherung bei deutschen Kritischen Infrastrukturen. Die Kenntnisnahme durch Unbefugte ist für die Interessen der Bundesrepublik Deutschland nachteilig.

Unter Abwägung zwischen dem parlamentarischen Auskunftsanspruch einerseits und dem Schutz von Sicherheitsinteressen der Bundesrepublik Deutschland unter Berücksichtigung der Geheimhaltung von Informationen zu Kritischen Infrastrukturen andererseits hat die Bundesregierung die erbetenen Informationen als Verschlusssache „VS – Vertraulich – amtlich geheimgehalten“ eingestuft. Die Antwort der Bundesregierung ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung des Deutschen Bundestages eingesehen werden.

10. Wie viele Beamte des BSI sowie weitere Beamte und Angestellte des Bundes sind mit der Überprüfung dieser Vorkehrungen betraut?

    Wie viele KRITIS-Prüfer gibt es?

Die erbetenen Informationen zur personellen Ausstattung können nicht öffentlich zur Verfügung gestellt werden. Unbefugte würden die Möglichkeit erhalten, aus diesen Daten Rückschlüsse zu ziehen, die einzeln oder in ihrer Kombination eine Gefahr für Einrichtungen der Kritischen Infrastrukturen alleine oder in der Gesamtheit darstellen. Aus dem Vergleich der genannten Mitarbeiterzahlen mit Mitarbeiterzahlen anderer Bereiche ließen sich Rückschlüsse auf die Schwerpunktsetzung des BSI ziehen.

Unter Abwägung zwischen dem parlamentarischen Auskunftsanspruch einerseits und dem Schutz von Sicherheitsinteressen der Bundesrepublik Deutschland unter Berücksichtigung der Geheimhaltung von Informationen zu Kritischen Infrastrukturen andererseits hat die Bundesregierung die erbetenen Informationen als Verschlusssache „VS – Vertraulich – amtlich geheimgehalten“ eingestuft. Die Antwort der Bundesregierung ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung des Deutschen Bundestages eingesehen werden.

11. Wurden oder werden im Rahmen des Themas „Kritische Infrastruktur“ Beratungsleistungen oder sonstige externe Leistungen eingeholt, und wenn ja, durch wen, in welcher Form, und zu welchen Kosten (bitte einzeln aufschlüsseln)?

Die erbetenen Informationen zu Beratungs- oder Unterstützungsleistungen können nicht öffentlich zur Verfügung gestellt werden. Unbefugte würden die Möglichkeit erhalten, aus diesen Daten Rückschlüsse zu ziehen, die einzeln oder in ihrer Kombination eine Gefahr für Einrichtungen der Kritischen Infrastrukturen alleine oder in der Gesamtheit darstellen.

Eine Übersicht über vom BSI beauftragte Studien ermöglicht Rückschlüsse auf im Fokus des BSI stehende Sektoren oder Bereiche. Die Kenntnisnahme durch Unbefugte ist für die Interessen der Bundesrepublik Deutschland nachteilig.

Unter Abwägung zwischen dem parlamentarischen Auskunftsanspruch einerseits und dem Schutz von Sicherheitsinteressen der Bundesrepublik Deutschland unter Berücksichtigung der Geheimhaltung von Informationen zu Kritischen Infrastrukturen andererseits hat die Bundesregierung die erbetenen Informationen als Verschlusssache „VS – Vertraulich – amtlich geheimgehalten“ eingestuft. Die Antwort der Bundesregierung ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung des Deutschen Bundestages eingesehen werden.

12. Welchen Standards und technische Richtlinien müssen die Verwahrung von Daten über oder aus Kritischer Infrastruktur erfüllen?

Die Bundesregierung schützt die Daten gemäß gesetzlichen und rechtlichen Bestimmungen und setzt die dafür erforderlichen technischen und organisatorischen Maßnahmen um.

13. Sind diese Standards für die Datenverwahrung auf Seiten des Bundes beziehungsweise von bundeseigenen Unternehmen nach Kenntnis der Bundesregierung bisher gewahrt worden?

Der Bundesregierung sind in diesem Zusammenhang keine Verstöße gegen gesetzliche und rechtliche Bestimmungen bekannt.

Gesamtherstellung: H. Heenemann GmbH & Co. KG, Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333